

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE		READ INSTRUCTIONS BEFORE COMPLETING FORM												
1. REPORT NUMBER TOP 1-1-060	2. GOVT ACCESSION NO.	3. RECIPIENT'S CATALOG NUMBER												
4. TITLE (and Subtitle) U.S. ARMY TEST AND EVALUATION COMMAND TEST OPERATIONS PROCEDURE "SYSTEM SAFETY ENGINEERING"		5. TYPE OF REPORT & PERIOD COVERED												
7. AUTHOR(s)		6. PERFORMING ORG. REPORT NUMBER												
9. PERFORMING ORGANIZATION NAME AND ADDRESS U.S. ARMY COMBAT SYSTEMS TEST ACTIVITY (STECs-AD) ABERDEEN PROVING GROUND, MD 21005-5059		8. CONTRACT OR GRANT NUMBER(s)												
11. CONTROLLING OFFICE NAME AND ADDRESS U.S. ARMY TEST AND EVALUATION COMMAND (AMSTE-TC-M) ABERDEEN PROVING GROUND, MD 21005-5055		10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS												
14. MONITORING AGENCY NAME & ADDRESS (if different from Controlling Office)		12. REPORT DATE 7 April 1986												
		13. NUMBER OF PAGES												
		15. SECURITY CLASS. (of this report) Unclassified												
		15a. DECLASSIFICATION DOWNGRADING SCHEDULE												
16. DISTRIBUTION STATEMENT (of this Report)  Approved for public release; distribution unlimited.														
17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)														
18. SUPPLEMENTARY NOTES														
19. KEY WORDS (Continue on reverse side if necessary and identify by block number) <table border="0"> <tr> <td>Fault tree analysis</td> <td>Hazard severity</td> <td>System hazard analysis,</td> </tr> <tr> <td>Hazard analysis</td> <td>Preliminary hazard analysis</td> <td></td> </tr> <tr> <td>Hazard classification</td> <td>Probability</td> <td>System safety</td> </tr> <tr> <td>Hazards</td> <td>Safety assessment report,</td> <td>System/subsystem. ←</td> </tr> </table>			Fault tree analysis	Hazard severity	System hazard analysis,	Hazard analysis	Preliminary hazard analysis		Hazard classification	Probability	System safety	Hazards	Safety assessment report,	System/subsystem. ←
Fault tree analysis	Hazard severity	System hazard analysis,												
Hazard analysis	Preliminary hazard analysis													
Hazard classification	Probability	System safety												
Hazards	Safety assessment report,	System/subsystem. ←												
20. ABSTRACT (Continue on reverse side if necessary and identify by block number) <p>Provides guidance for identifying and evaluating hazards associated with systems being tested by U.S. Army Test and Evaluation Command (TECOM). The purpose of this TOP is to provide uniform requirements and criteria for performing system safety analysis during the course of testing materiel. Each test program must be designed to ensure that pertinent safety specifications and criteria are verified and to identify unknown hazards or procedures which may have been designed into the systems. Testing will provide determination</p>														

DD FORM 1 JAN 73 1473 EDITION OF 1 NOV 65 IS OBSOLETE

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

86 6 17 060

AD-A168 737

DMC FILE COPY

UNCLASSIFIED

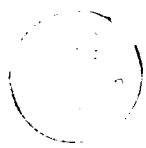
SECURITY CLASSIFICATION OF THIS PAGE(When Data Entered)

or assessment of personnel and equipment hazards in the system and associated operation and maintenance hazards.

Pertinent data from all tests will be used to provide a basis for evaluating safety and health characteristics. Specific safety tests will be performed on critical devices or components to determine the nature and extent of hazards presented by the materiel.

X

A-1



UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE(When Data Entered)

U.S. ARMY TEST AND EVALUATION COMMAND  
TEST OPERATIONS PROCEDURE

AMSTE-RP-702-100

Test Operations Procedure (TOP) 1-1-060  
AD No.

7 April 1986

SYSTEM SAFETY ENGINEERING

	<u>Page</u>
Paragraph 1. SCOPE. . . . .	1
2. FACILITIES AND INSTRUMENTATION . . . . .	1
3. REQUIRED TEST CONDITIONS . . . . .	2
4. TEST PROCEDURES. . . . .	3
5. PRESENTATION OF DATA . . . . .	10
Appendix A BACKGROUND . . . . .	A-1
B METHODS OF HAZARD IDENTIFICATION . . . . .	B-1
C INSPECTION/OBSERVATION CHECKLISTS. . . . .	C-1
D HAZARD SEVERITY AND CLASSIFICATION . . . . .	D-1
E SAFETY RELATED TOPS. . . . .	E-1
F REFERENCES . . . . .	F-1

1. SCOPE. This TOP provides guidance for identifying and evaluating hazards associated with systems being tested by U.S. Army Test and Evaluation Command (TECOM). The purpose of this TOP is to provide uniform requirements and criteria for performing system safety analysis during the course of testing materiel. Each test program must be designed to ensure that pertinent safety specifications and criteria are verified and to identify unknown hazards or procedures which may have been designed into the systems. Testing will provide determination or assessment of personnel and equipment hazards in the system and associated operation and maintenance hazards.

Pertinent data from all tests will be used to provide a basis for evaluating safety and health characteristics. Specific safety tests will be performed on critical devices or components to determine the nature and extent of hazards presented by the materiel.

2. FACILITIES AND INSTRUMENTATION.

2.1 Facilities. The facilities used during a system safety subtest are diverse and are, therefore, listed in the specific TOPs (See TOP index.<sup>2</sup>) which cover the materiel under test.

2.2 Instrumentation. Because of the wide variety of commodity items, it is not feasible to include an exhaustive list of all necessary instrumentation. The actual instrumentation will be determined by the equipment under evaluation.

<sup>1</sup>Reference numbers match those in Appendix F, References.

### 3. REQUIRED TEST CONDITIONS.

3.1 Test Plans. Test plans will be written according to TECOM Regulation 70-24.<sup>3</sup> A subtest entitled "Safety and Health Evaluation" will be included in the written test plan for all tests, to include objective(s), criteria, data required, data acquisition procedure, and analytical procedure.

3.2 Distribution of Test Reports. Test reports will be distributed according to TECOM Regulation 70-24. Additionally, copies of the test plans should be made available to support groups involved in the systems testing.

3.3 Test Reports. A "Safety and Health Evaluation" section shall/must be included in Section 2 of formal test reports and in the summary of results paragraph of letter reports. This subtest should follow the format outlined in TECOM Regulation 70-24. This evaluation shall identify all real or potential safety and health hazards that occurred or were observed during the test. It is important to identify and evaluate all hazards in this section of the report, so that they receive proper consideration as hazards, and not exclusively as performance shortcomings. To avoid unnecessary repetition, it is appropriate to list the hazards and their classifications in the safety and health section, and to reference the specific paragraphs in other sections of the report rather than to repeat detailed information.

### 3.4 Preliminary Safety Review and Documentation Preparation.

a. Ensure that a safety assessment report (SAR) has been received from the developer as required by AR 385-16.<sup>4</sup> All developer/contractor-identified safety and health hazards should be documented in the SAR. Ensure that systems that may present health hazards have been evaluated and a health hazard assessment report submitted in accordance with AR 40-10.<sup>5</sup> All safety and health hazards identified must be taken into account, classified in accordance with MIL-STD-882B,<sup>6</sup> and included in the safety and health section of the test report.

b. Ensure that all required Test Operations Procedures (TOPs) and Standing Operating Procedures (SOPs) are available. The procedures for all hazardous operations should be documented in the SOPs. SOPs or supplements are prepared for specific tests of individual items whenever general SOPs do not apply.

c. Ensure that specific tests are included in the test plan to verify compliance with safety and health criteria.

d. Review appropriate regulations which deal with specific tests.

e. Review the system support package, all instructional material, literature, and draft manuals. Be sure that instructions to avoid hazardous situations are well documented.

### 3.5 Training and Familiarization.

a. Ensure that required training is conducted by the developer.

b. Conduct a preoperational briefing for all personnel prior to the start of the test. All personnel will review the hazards and precautions outlined in

the SAR and SOP. Be sure that all personnel are wearing the required personal protective equipment.

**3.6 Safety Inspection.** A safety inspection of the test item shall be performed by qualified test personnel prior to beginning the test. Safety engineering assistance may be requested, as required, through the safety office. Appropriate checklists may be available by referring to specific TOPs, or may be developed for application of unique systems.

a. Prompt detection and correction of unsafe conditions are an absolute must throughout the life cycle of military systems. There are three major causes of unsafe conditions. The end result of the three listed below is a steady trickle of unsafe conditions into almost every system.

- (1) Unsafe design of systems or subsystems including software.
- (2) Wear and tear process that is always at work.
- (3) Unsafe conditions caused by personnel who use or maintain the systems.

b. There are two kinds of inspections.

(1) Incidental inspection. This type of inspection is ongoing. Test personnel should look for unsafe conditions continuously as they perform all of the required testing.

(2) The planned inspection. This type of inspection is deliberate and thorough. The testers should know in advance what specific items to inspect and what conditions to look for. This inspection should be performed before and at the conclusion of testing.

c. Inspection checks and analysis. When a system is analyzed for inspection purposes, testers should look closely at those items which can result in unsafe conditions.

d. Inspection checklists.

(1) Inspection checklists that cover common types of unsafe conditions are listed in Appendix C.

(2) Inspection checklists which cover specific systems may be found in the TOPs used to test those systems.

(3) When the checklists, as described above, do not adequately cover the system or subsystem in question, appropriate checklists can be developed as described in Appendix C.

**4. TEST PROCEDURES.** Test procedures may vary depending on the system being tested. Specific safety and health evaluation subtests will be designed to evaluate all safety and health criteria established for an item or to otherwise identify hazards. The subtests are usually described in the TOP for the specific commodity being tested. A comprehensive subtest will be designed to establish the safety of the item/system including the following essential features:

a. Preliminary examinations and limited tests necessary to certify that the item/system is safe for testing.

b. Selected physical performance and reliability tests to verify that the item/system under test satisfies minimum design and construction requirements for safe field deployment.

c. Systematic observation and analysis of the test system throughout all phases of development testing to identify and investigate any actual or potential hazards to personnel and equipment that may result from operation and maintenance of the system by representative users.

d. Criteria for safety evaluation subtests will be drawn, when possible, from the applicable requirements document. In the absence of specific criteria in said document, however, the following may be used: "The system shall be designed to incorporate sound system safety engineering principles according to MIL-STD-882B. Safety and health hazards shall be eliminated or otherwise minimized throughout the entire life cycle of the system in accordance with appropriate guidance documents."

e. Test directors must ensure that support groups include system safety evaluations when performing specific subtests. Data presented to the test directors should include identified hazard interfaces which could result in hazardous failures.

#### 4.1 Methods.

4.1.1 Hazard Identification and Analysis. The equipment operation hazards analysis is based upon the results of all subtests that may contain information concerning the safety and health characteristics of the test system. Based upon the results of the safety inspection(s), hazard analysis, test results, comments from operating and maintenance personnel, and a review of all appropriate literature, the following hazards should be considered for evaluation using the techniques and checklists described in Appendix C:

- a. Mechanical hazards.
- b. Electrical hazards.
- c. Chemical hazards.
- d. Health hazards.
- e. Fire hazards.
- f. Explosive hazards.
- g. Procedural hazards (operating and maintenance).
- h. Software hazards.

#### 4.1.1.1 Mechanical Hazards.

a. Carefully examine all instructional material to determine potential mechanical hazards.

b. Accomplish a thorough test-item safety inspection, and observe the item throughout all test and evaluation phases. Solicit the comments and observations of equipment operators and other support personnel.

c. Consider the following potential mechanical hazard sources when performing this evaluation:

- (1) Rotating, reciprocating and transverse motions.
- (2) Cam action.
- (3) Cutting actions--motion.
- (4) Cutting exposure--sharpness.
- (5) Punching, shearing, and bending actions.
- (6) Rate of speed.
- (7) Instability (center of gravity).
- (8) Entrapment.
- (9) Lack of clearance.
- (10) Misleading appearance of quality.
- (11) Stored energy--physical.
- (12) Improper rigidity.
- (13) Impact.

d. A sample checklist and methods of safeguarding against mechanical hazards are included in Appendix C.

#### 4.1.1.2 Electrical Hazards.

a. Examine all instructional material; determine the location of all potential electrical hazards, and ensure that these hazards are clearly indicated and that appropriate precautionary notices and instructions are provided.

b. Thoroughly inspect the test item for safety during the initial safety inspection and during all phases of testing and evaluation.

c. Obtain comments and observations from equipment operators.

d. Consider the following electrical hazard sources when performing this evaluation:

- (1) Shock.
- (2) Short circuit.
- (3) Stored electrical charge (batteries and stray voltage).
- (4) Improper and/or inadequate ground.
- (5) Fire.
- (6) Overheating.
- (7) Ventilation.
- (8) Insulation failure.
- (9) Sparks.
- (10) Arcing.
- (11) Explosion.

e. A sample checklist upon which a safety evaluation of electrical hazards can be performed is included in Appendix C.

#### 4.1.1.3 Chemical Hazards.

a. Determine each chemical contained in or used with this equipment. Obtain and review a copy of the material safety data sheet (MSDS) from the manufacturer or developer for each chemical involved with the system.

b. When exposure of personnel to chemicals will occur during operation of the system, ensure that the health hazards for each chemical have been considered and that controls are employed to ensure maximum allowable exposure limits are not exceeded. If protective devices are used to eliminate or control the exposure, their adequacy must be evaluated.

c. In addition, review each chemical for the following properties and their effects on the system/personnel:

- (1) Corrosion.
- (2) Toxicity due to the following:
  - (a) By inhalation.
  - (b) By skin absorption.
  - (c) By ingestion.
- (3) Flammability.
- (4) Explosive limits.



- (5) Physical stress.
- (6) Temperature--variation and extremes.
- (7) Oxygen depletion.
- (8) Lifting and carrying.
- (9) Toxic gases and particulates (TOP 2-2-614<sup>9</sup>).

e. A sample checklist upon which an evaluation of health hazards can be performed is included in Appendix C.

#### 4.1.1.5 Fire and Explosion Hazards.

a. Accomplish a thorough test-item inspection, and observe the item throughout all tests and evaluations for fire and explosion hazards.

b. The following fire- and explosion-related hazards should be considered:

- (1) Fuel source.
- (2) Rate of flammability.
- (3) Ignition source resulting from the following:
  - (a) Heat (chemical).
  - (b) Heat (spontaneous).
  - (c) Heat (mechanical).
  - (d) Heat (electrical).
  - (e) Spark (mechanical).
  - (f) Spark (electrical-static).
  - (g) Open flame.

c. A sample checklist upon which to base an evaluation of fire and explosion hazards is included in Appendix C.

#### 4.1.1.6 Explosives and Ammunition.

a. Volume 4 of the Index of Test Operations Procedures covers the testing of ammunition and explosives. This category includes ammunition for artillery, tanks, recoilless rifles, mortars, small arms, and aircraft weapons; small rockets and missiles; mines; demolition equipment; pyrotechnics; grenades; and flame throwers.

b. The provisions of AMC Regulation 385-100<sup>10</sup> apply to the safety of all testing.

- (5) Shock sensitivity.
- (6) Oxidation.
- (7) Photosensitivity.
- (8) Reactivity with water, air, fuels and lubricants, materials of construction.
- (9) Carcinogenicity.
- (10) Susceptibility to decomposition.

d. A sample checklist upon which a safety and health evaluation of chemical hazards can be performed is included in Appendix C.

#### 4.1.1.4 Health Hazards.

a. Throughout the conduct of the test, note any conditions that might be physiologically hazardous to operation or maintenance personnel.

b. Make specific industrial hygiene measurements to verify suspected hazards.

c. Arrangements for assistance may be made through the safety office.

d. Consider the following sources of health hazards:

- (1) Noise (pressure) from the following:
  - (a) High intensity.
  - (b) High frequency.
  - (c) Impulsive.
- (2) Vibration.
- (3) Radiation, ionizing.
- (4) Radiation, nonionizing from the following:
  - (a) Ultraviolet emission.
  - (b) Visible-light emission.
  - (c) Infrared emission.
  - (d) Microwave emission.
  - (e) Radiowave emission.
  - (f) Lasers.

#### 4.1.1.7 Procedural Hazards.

a. Personnel errors. Personnel are injured and systems are lost due to procedural errors.<sup>11</sup> Systems safety techniques should be used to foresee human error so that appropriate design changes and/or appropriate training can be developed. Potential hazards exist in the operation and maintenance functions during the life cycle of the systems.

b. Maintenance planning: Hazards resulting from inadequate maintenance need to be foreseen. It is important that the reliability data collected for critical system components (e.g., brakes) be utilized to establish scheduled maintenance tasks in order to lessen the deterioration of safety to unacceptable levels. Individual failure modes and their interfaces need to be addressed.

#### 4.1.1.8 Software Hazard Analysis.

a. When test item/system includes operations that are controlled by software/computers, a software/computer hazard analysis to identify hazardous conditions incident to safety critical operator information and command and control functions should be performed according to TOP 1-1-056.<sup>12</sup>

b. The software/computer hazard analysis should examine software/computer and its system interfaces for events, faults, and occurrences such as timing which could cause or contribute to hazardous events affecting safety. This effect shall be accomplished by tracing safety-critical operator information and commands through source/object code, through system simulation, and through other applicable documentation. Safety-critical programs/modules should be analyzed for sensitivity to software or hardware failures which could cause the system to operate in a hazardous manner (MIL-STD-882B).

4.1.2 Preliminary Hazard Analysis (PHA). The preliminary hazard analysis is the initial effort which shall be performed by the contractor or developer during the system design phase. It is the first hazard search to be performed on the system. The PHA should be included in the safety assessment report for each system to be tested. The PHA should include, but not be limited to, the following activities:

- a. Review pertinent historical safety experience data.
- b. List categorically basic hazard sources including an identification of possible causes in each category.
- c. Investigate the various sources to determine the provisions which have been developed for their control.
- d. Identify hazard sources for which inadequate controls have been provided in the proposed design/procedures.
- e. Provide specific safety requirements/criteria which should be incorporated into the program documentation to ensure control of the sources which present unacceptable hazard levels.

4.1.3 Subsystem Hazard Analysis (SSHA). The purpose of the SSHA is to identify hazards associated with design of subsystems including component failure modes,

critical human error inputs, and hazards resulting from functional relationships between components and equipment comprising each subsystem.

**4.1.4 System Hazard Analysis (SHA).** The purpose of the SHA is to identify and assess existing or potential hazards between subsystems and systems and their effects on overall system safety and operations. The emphasis is on interfaces. Through the early identification of existing or potential hazards, corrective action can be taken to eliminate or control hazard categories I and II and minimize or control hazard categories III and IV (ref MIL-STD-882B).

An SHA should be conducted on the critical interrelationships of each subsystem and system to determine the cause and effect of possible independent, dependent, and simultaneous failures that could present a hazardous condition including failure of safety devices. A well documented analysis shows compliance with specified safety and operational requirements. Instructions for performing an SHA are included in Appendix B.

a. Prepare a critical items list (CIL) of all safety-critical items to provide visibility for immediate corrective action to prevent personal injury or system damage when a category I or II hazard is identified (MIL-STD-882B). CIL instructions are included in Appendix B.

b. Identify specific hazards from the CIL that need further analysis to determine the combination of causes that may lead to these hazardous events. A fault tree analysis (FTA) is an ideal methodology for the identification of occurrences that will lead to the undesired event. (Instructions and procedures for conducting an FTA are included in the Appendix B.) Assistance from a system safety engineer may be advisable.

c. Classify all identified hazards according to Appendix D.

d. Use data from reliability tests to determine level of safety in a subsystem (e.g., mean time between failures (MTBF) of brake system).

#### **4.2 Data Required.**

a. Include copies of checklists, PHA, SSRA, CIL, and FTA in the appendix of the report.

b. Include data from specific subtests that are related to safety such as toxic fumes tests, brake tests, etc. Statistical data should be listed if it is safety related.

c. Include data from measured conditions that impact safety (i.e., electrical energy, pressures, temperature, noise, etc.).

d. Include photographs to clarify the nature of the hazard.

e. Include other data required by the Independent Evaluation Plan (IEP) and Test Design Plan (TDP) from higher headquarters.

**5. PRESENTATION OF DATA.** Sufficient narrative comments will be included on each condition to provide background information to be used in the analysis of test results.

a. Specific procedures for reducing and presenting data are usually explained in the specific TOPs used in the performance of each subtest. Due to the fact that most subtests are not conducted to singularly evaluate safety and health aspects of the systems, each subtest must be reviewed to recognize the safety and health implications of the test results. From this review, a concise listing of all existing and potential hazards shall be compiled and listed in the safety and health evaluation of the test report. The potential consequence of each hazard shall be considered concurrently.

b. Each hazard is to be categorized with respect to severity and probability according to the provisions of MIL-STD-882B. Each system characteristic that creates a hazard is then classified in accordance with Appendix D.

c. Work sheets used to conduct hazard analysis should be included in the appendix of the test report.

d. Safety confirmation of items/systems such as ammunition, weapons, etc. is dependent on data obtained from limited sample sizes. It is, therefore, important that the use and application of inference statistics be considered during the planning stage of every test. Assistance can also be obtained from a statistical analyst.

e. List recommended changes in design and/or procedures that would change hazard classifications to the acceptable level.

f. List all hazards classified as deficiencies, shortcomings, and suggested improvements according to MIL-STD-882B.

Recommended changes to this publication should be forwarded to Commander, U.S. Army Test and Evaluation Command, ATTN: AMSTE-TC-M, Aberdeen Proving Ground, MD 21005-5055. Technical information may be obtained from the preparing activity, Commander, U.S. Army Combat Systems Test Activity, ATTN: STECS-AD, Aberdeen Proving Ground, MD 21005-5059. Additional copies are available from the Defense Technical Information Center, Cameron Station, Alexandria, VA 22304-6145. This document is identified by the accession number (AD No.) printed on the first page.

## APPENDIX A

BACKGROUND

The principal objective of a system safety program within the Department of Defense is to ensure that safety, consistent with mission requirements, is designed into systems, subsystems, equipment, and facilities. A formal safety program that stresses early hazard identification and elimination or control is the principal contribution of effective system safety (MIL-STD-882B).

The primary objectives of system safety follow:

- a. Maximize operational readiness and mission protection by ensuring that appropriate hazard-control measures are designed into the system in a timely manner and at minimum cost.
- b. Ensure each safety and health risk for new designs, materials, and production/construction and testing techniques are either controlled or that risk is formally accepted and documented.
- c. Reduce retrofit requirements.

System safety will be applied and tailored to all Army systems or facilities throughout their respective life cycles. System safety engineering and management will also be applied during basic technology development. For systems developed by private industry, depots, other services, or foreign governments, application of system safety will begin when the decision is made to evaluate the system for Army use. Acquisition programs for Army systems include system safety requirements tailored according to the severity of related hazards and the potential for accidents.

No compromises of system safety criteria will be made without formal documentation of the accepted risks. The documentation for risk acceptance will be approved by the Army acquisition executive or other designated acquisition manager.

Most accidents are quite complex from a causal standpoint. It is the common tendency to oversimplify that makes many accidents appear to have only one cause. There are almost always a number of causes that have acted in sequence and in combination to cause an accident. The two most important causes of accidents are personnel and environment.

## APPENDIX B

METHODS OF HAZARD IDENTIFICATION

Timely identification of a hazard is the initial step needed to conduct safety analysis. Effective hazard analysis requires a systematic approach.

Begin by reviewing the operational mode of the system. Then describe the most probable sequence of undesirable events (accident scenario) that could result. Undesirable events may include, among other things, system failure and malfunctions, human errors, environmental conditions, improper system configurations, and safeguard failures. To identify each hazard, it is necessary to foresee the events that may lead to accidental injury or system loss. The hazards can be classified by basic types of potential accidents. The test directors or others performing the hazard analysis should answer the following questions:

Can someone be struck-by (SB) some moving object in the system? A struck-by accident is one in which a person has been contacted abruptly and forcefully by some object in motion. Things that strike people fall into three broad categories:

- Normally moving objects
- Normally stationary objects
- Extreme pressures (explosion, etc.).

Can someone strike against (SA) some object? A struck-against accident is one in which a person contacts abruptly, and with force some object. Things that produce struck-against accidents are:

- Protruding objects
- Permanent objects requiring an effort to avoid
- Cramped or congested work areas
- Applying great manual force to anything.

Can someone be caught between (CBE) two or more objects? A caught-between accident is one in which a person is pinched, crushed, or otherwise caught between either a moving object and a stationary object or between two moving objects. Three general situations contribute to caught-between accidents:

- A normally moving object approaching or contacting a stationary object.

- Two normally moving objects approaching or contacting each other.

- A normally stationary object that is caused to move so that it approaches or contacts a stationary object.

Can someone be contacted by (CBY) or contacted with (CW) some substance that can cause injury on contact? A contacted-by accident is one in which a person has been contacted by some substance that can cause injury on contact. A contact-with accident is one in which a person has contacted some substance or object capable of producing injury on the basis of nonforceful contact alone. Situations which are likely to result in contact-by or contact-with accidents are:

Equipment containing injurious materials  
Electrically charged equipment  
Hot or cold material  
Corrosive chemicals.

Can someone fall below (FB) or fall to the same level (FS)? A fall is an accident in which a person either falls to a level below the one on which the person was standing or falls onto the same level on which he/she was standing.

Can someone be exposed (E) to some harmful condition that might cause injury or illness? An exposure accident is one in which a person suffers injury or illness as a result of exposure to harmful conditions. Six conditions account for most exposure accidents:

Toxic gases, fumes or vapors  
Toxic airborne particles  
Extremes of heat or cold  
Oxygen-deficient atmosphere  
Radioactive radiation  
Intense light.

Can someone be over-exerted (O)? An over-exerted strain accident is one in which a person sustains an injury by putting excessive strain on some part of the body. The three common work situations that cause most over-exertion accidents are:

Manually handling heavy objects  
Using extreme force to release something stuck  
Attempting to recover unbalanced equipment.

Can someone be caught in (CI) or caught on (CO) something to cause injury? A caught-in accident is one in which an employee or some part of the body is trapped or caught in some type of enclosure or opening. A caught-on accident is one in which a person (or some part of a person's clothing) is caught on a protruding object.

Three situations that often result in caught-in accidents are:

Working in single-entry enclosures  
Exposure to small floor openings  
Working in very tight places.

Two basic environmental conditions that often cause caught-on accidents are:

A stationary projecting object  
A moving projecting object.

To assist in the hazard identification, checklists included in this TOP should be used. Additional checklists may be available in other sources.

#### System Safety Analytical Techniques.

General. Of the various tasks or jobs to be accomplished in the system safety effort, the requirement to conduct system safety analyses is one of the most



important. Utilization of the modern system safety analytical technology which has been developed will provide the key element in the system engineering process. It should be recognized that only a limited amount of useful data is available to the system safety analyst. It is, therefore, imperative that the data be used in the most logical and comprehensive manner in order to provide an effective product. In the final analysis, system safety management must be provided for maximum visibility relative to the risks which will be assumed during a given system operation.

**System analysis.** A basic understanding of the system-analysis process in general, or evaluation of systems utilizing the "systems" concept is required. This understanding is necessary prior to the presentation of specific system safety analytical techniques. System analysis is defined as a directed process for the orderly acquisition of specific information pertinent to a given system. For a system safety analysis, we are, therefore, directed toward the acquisition of pertinent safety information relative to the given system. The many different types of system analysis are categorized into three basic groups which are:

Intuition which is defined as the immediate knowing or learning of something without the conscious use of logical reasoning. The intuitive approach to safety analysis can best be summarized by the statement, "We build safe systems."

Induction which is defined as logical reasoning from particular facts to a general conclusion. An example of the use of inductive method of system analysis would be an examination of the failure characteristics of the components of a system and the determination of the subsequent effects of these failures at the system level. A familiar application of this type of failure analysis is the failure mode and effects analysis (FMEA), which is commonly employed in reliability engineering programs. Similarly, the subsystem hazard analysis (SSHA) is an example of an inductive analytical process which is employed in system safety engineering programs.

Deduction which is defined as logical reasoning from the general to the specific. Deduction approaches the problem in an opposite direction, in comparison to the inductive process. An example of the use of the deductive method of system analysis would be the careful definition of a particular system-level event and a subsequent detailed examination of the components of the system to determine those which could contribute to the occurrence of the system-level event. Fault tree analysis is an example of a deductive analytical process which is employed in system safety engineering programs.

Summary of Modern System Safety Analytical Techniques. (These techniques are valuable tools in the testing community and are normally conducted by contractors and/or developers.)

System safety analysis should be a process which is fully capable of assuming a leading role in design analysis. The purpose of system safety analysis is to identify hazards in the system as it is proposed to be designed and operated, evaluate the risk associated with the hazards, and eventually to prevent or control the hazards which are considered to be unacceptable. In order to provide the analytical support required to analyze the postulated designs of systems, several methods of system safety analysis should be employed. These methods will be described in their chronological order of application during the system's life cycle.

One method is the preliminary hazard analysis (PHA) (reference Task 202 of MIL-STD-882B). Preliminary hazard analysis is used in the earliest phases of system design to identify known hazards such as energy sources. As detailed design information is available, the subsystem hazard analysis (SSHA) (reference Task 203 of MIL-STD-882B) is performed. The SSHA involves a detailed investigation of the system to determine component failure modes, various causes of failure, and the resultant effects on the safety of the system. Finally, the various procedures which are required to operate the system are reviewed by operating and support hazard analysis (O&SHA) (reference Task 205 of MIL-STD-882B).

These and other methods, which will be further described in the following paragraphs, should be performed to evaluate the hazardous conditions that may exist over a system's life cycle. The extent to which each method of analysis is applied should be mutually agreed upon by both contractor and customer, and so specified in the applicable system program plan. In specifying these specific analysis methods, it is not the intent to restrict the development and use of new methods.

Preliminary Hazard Analysis (PHA). (This is available in MIL-STD-882B and is normally performed by a contractor.)

This is an inductive process which should be conducted early in the design phase of the system life cycle to identify in broad or gross terms the potential hazards associated with the postulated operational concept. The analysis is a comprehensive, qualitative evaluation of the system which considers the system from the viewpoint of its operational environment. As potentially hazardous operations, materials, and design are identified, this information should be used in the development of safety criteria to be imposed in the performance/design specifications. The PHA, therefore, becomes a necessary system safety program element to provide assurance that the system safety requirements become an integral part of the overall technical design requirements.

The PHA should include, but not be limited to, the following activities:

- . A review of pertinent historical safety experience data.
- . A categorized listing of basic hazard sources including an identification of possible causes in each category.
- . An investigation of the various sources to determine the provisions which have been developed for their control.
- . Identification of hazard sources for which inadequate control has been provided in the proposed design/procedures.
- . The provision of specific safety requirements/criteria which should be incorporated into the program documentation to ensure control of the sources which present unacceptable hazard levels.

The following activities, areas, conditions should be considered when performing the PHA:

Hazardous components:

- . Hazardous materials
- . Energy sources
- . Fluids and oils
- . Off-property sources
- . Pressure systems.

Safety-related interface considerations among various elements:

- . EMI
- . Inadvertent activation
- . Fire/explosive initiation and propagation.

Environmental constraints:

- . Temperature extremes
- . Shock
- . Noise and health hazards
- . X-rays.

Construction constraints in addition to many of the environmental constraints are:

- . Transportation
- . Installation
- . Utilities
- . Laser radiation.

Operating, test and maintenance procedures:

- . Layout and lighting
- . Crash safety
- . Egress and rescue.

Facilities, support equipment and training:

- . Codes and standards
- . Certification
- . Storage, assembly and checkout.

Safety related equipment, safeguards:

- . Interlocks
- . Redundancy
- . Fail/safe design
- . Fire suppression systems
- . Personnel protective equipment.

TABLE B-1. HAZARD SEVERITY (MIL-STD-882B)

CATEGORY	DESCRIPTION	DEFINITION	OTHER DEFINITIONS
I	Catastrophic	Death or system loss	System out of service or severe impacts on revenue, O & M costs, program funding
II	Critical	Severe injury, severe occupational illness, or major system damage	Major damage costs or program delays
III	Marginal	Minor injury, minor occupational illness, or minor system damage	Minor damage costs or delays
IV	Negligible	Less than minor injury, occupational illness, or system damage	Routine repairs

TABLE B-2. PRELIMINARY HAZARD ANALYSIS (PHA)

Instructions for Completing Form:

In Contract No. \_\_\_\_\_, enter the contract number for which PHA is being performed.

In Contractor \_\_\_\_\_, enter the name of the contractor responsible for the PHA.

In PHA No. \_\_\_\_\_, enter the PHA number which shall be coded and sequentially numbered by each contractor for each system. This coding sequence will be utilized for all related analyses.

In Revision No. \_\_\_\_\_, enter the revision number to indicate the latest status.

In Subsystem \_\_\_\_\_, enter the nomenclature of the subsystem as broken out from the system.

In System \_\_\_\_\_, enter the nomenclature of the applicable system.

In Drawing No. \_\_\_\_\_, enter the number of the drawing on which the subsystem is indicated.

In Prepared by \_\_\_\_\_ Date \_\_\_\_\_, the preparer will sign and enter the date of issue or completion on each sheet of the analysis.

In Reviewed by \_\_\_\_\_ Date \_\_\_\_\_, the reviewer will sign and enter the date of review on each sheet of the analysis.

In Approved by \_\_\_\_\_ Date \_\_\_\_\_, the contractor's project manager will sign to approve and enter the date of approval on each sheet of analysis.

In (1) Function Description and No., enter the reference number and a brief functional description of the subsystem under analysis.

In (2) System Mode, enter the state of the system, at the time of the failure mode or condition.

In (3) Hazard Description, enter the nature of hazard condition introduced by the failure of the subsystem.

In (4) Potential Cause, enter the most likely primary and secondary causes of the hazard condition.

In (5) Effect on Subsystem/Interfacing Subsystems, enter a brief description of the hazard condition effect(s) on the subsystem and other interfacing subsystems.

In (6) Hazard Category, enter the highest applicable hazard class in accordance with MIL-STD-882B.

In (7) Redesign/Control Remarks, enter a brief description of the redesign/control/corrective action(s) necessary for the hazard condition being analyzed. Enter name(s) of related analysis and reference number(s) and which approach is being proposed - design change, procedures, special training, etc.



Subsystem Hazard Analysis (SSHA).

The SSHA is an inductive process which, in effect, is an expansion of, with increased complexity over, the preliminary hazard analysis. The completion of this analysis will normally occur during the design phase and prior to the design freeze (in a system development, prior to CDR). This occurs when the actual system design has been refined to the point where the detailed information is available. It can be used effectively, however, during operations as part of an investigation to establish cause-and-effect relationships and probabilities.

There are several types of SSHA's:

- Fault hazard analysis (FHA)
- Sneak circuit analysis
- Fault tree analysis (FTA).

Only the FHA and FTA, however, are discussed herein.

An SSHA/FHA is conducted on identified failure modes, and will be qualitative to a quantitative analysis as the design develops. When the analysis indicates a potential problem, it should be made known to the responsible engineer in order to initiate proper action. An FHA should be reviewed on a continuous basis to ensure that design modifications do not add hazards to the system. The FHA should be developed in conjunction with the failure modes, effects and criticality analysis (FMECA).

It provides information to evaluate identified hazards, identifies safety critical areas and provides inputs to safety design criteria and procedures with provisions and alternatives to eliminate or control all category I and II hazards, to minimize or control category III and IV hazards, and to identify critical items.

TABLE B-3. FAULT HAZARD ANALYSIS (FHA)

Instructions for Completing Form:

In Contract No. \_\_\_\_\_, enter the contract number for which FHA is being performed.

In Contractor \_\_\_\_\_, enter the name of the contractor responsible for the FHA.

In FHA No. \_\_\_\_\_, enter the FHA number which shall be coded and sequentially numbered by each contractor for each system. This coding sequence will be utilized for all related predictions and analyses.

In Revision No. \_\_\_\_\_, enter the revision number to indicate the latest status.

In Subsystem \_\_\_\_\_, enter the nomenclature of the subsystem as broken out from the system and which includes the item undergoing FHA.

In System \_\_\_\_\_, enter the nomenclature of the applicable system.

In Drawing No. \_\_\_\_\_, enter the number of the drawing on which the LRU is indicated.

In Prepared by \_\_\_\_\_ Date \_\_\_\_\_, the preparer will sign and enter the date of issue or completion on each sheet of the analysis.

In Reviewed by \_\_\_\_\_ Date \_\_\_\_\_, the reviewer will sign and enter the date of review on each sheet of the analysis.

In Approved by \_\_\_\_\_ Date \_\_\_\_\_, the contractor's project manager will sign to approve and enter the date of approval on each sheet of analysis.

In (1) LRU No. and Description, enter the reference number nomenclature and brief functional description of the component/assembly.

In (2) Failure Mode, enter a brief description of the failure or condition that is being analyzed.

In (3) Failure Rate, enter the probability of occurrence of failure mode or condition. Give data source, such as experience, GIDEP, MIL-HBK-217.

In (4) System Mode, enter the state of the system when the failure mode or condition occurs.

In (5) Cause, enter the most likely primary and secondary causes of the failure mode or condition.

In (6) Effect on Subsystem, enter a brief description of the failure mode or condition effect(s) on the assembly or next higher level assembly inputs and outputs; and in Effect on System, enter a brief description of the failure mode or condition effect(s) on the system and operations.

In (7) Hazard Category, enter the highest applicable hazard class in accordance with MIL-STD-882B.

In (8) Redesign/Control Remarks, enter a brief description of the redesign/control/corrective action(s) necessary for the failure mode or condition being analyzed. Enter name(s) of related analysis/analyses and reference number(s).





System Hazard Analysis (SHA).

The purpose of the SHA is to identify and assess existing or potential hazards between subsystems and systems and their effects on overall system safety and operations. The emphasis is on interfaces. Through the early identification of existing or potential hazard(s), corrective action can be taken to eliminate or control hazard categories I and II and minimize or control hazard categories III and IV.

An SHA is conducted on the critical interrelationships of each subsystem and system to determine the cause and effect of possible independent, dependent and simultaneous failures that could present a hazardous condition including failures of safety devices. When the SHA indicates a potential problem, it should be made known to the responsible engineer in order to initiate a design review. The SHA should be reviewed on a continuous basis to ensure that design modifications do not add hazards to the system.

The SHA helps ensure that all possible hazards associated with subsystem and system failure will be identified and corrective action taken. The SHA results are useful inputs to design reviews, maintainability, reliability and system safety and system operations.

A well-documented analysis shows compliance with specified safety and operational requirements and is a key part of the certification process.

TABLE B-4. SYSTEM HAZARD ANALYSIS (SHA)

Instructions for Completing Form:

In Contract No. \_\_\_\_\_, enter the contract number for which SHA is being performed.

In Contractor \_\_\_\_\_, enter the name of the contractor responsible for the SHA.

In SHA No. \_\_\_\_\_, enter the SHA number which shall be coded and sequentially numbered by each contractor for each system. This coding sequence will be utilized for all related productions and analyses.

In Revision No. \_\_\_\_\_, enter the revision number to indicate the latest status.

In System \_\_\_\_\_, enter the nomenclature of the applicable system.

In Drawing No. \_\_\_\_\_, enter the number of the drawing on which the subfunction is indicated.

In Interfacing System \_\_\_\_\_, enter the nomenclature of the applicable interfacing system.

In Prepared by \_\_\_\_\_ Date \_\_\_\_\_, the preparer will sign and enter the date of issue or completion on each sheet of the analysis.

In Reviewed by \_\_\_\_\_ Date \_\_\_\_\_, the reviewer will sign and enter the date of issue or completion on each sheet of the analysis.

In Approved by \_\_\_\_\_ Date \_\_\_\_\_, the contractor's project manager will sign to approve and enter the date of approval on each sheet of the analysis.

In (1) Hazard Description, enter the nature of hazard condition introduced by the failure of the system.

In (2) System Mode, enter the state of the system instants before the failure mode or condition.

In (3) Potential Cause, enter the most likely primary and secondary causes of the hazard condition.

In (4) Effect(s) on System, enter a brief description of the hazard condition effect(s) on the system.

In (5) Effect(s) on Interfacing System(s), enter a brief description of the hazard condition effect(s) on the interfacing system(s).

In (6) Interfacing Parameters, enter the parameters responsible for the interfacing of the system with other systems.

In (7) Hazard Category, enter the highest applicable hazard class in accordance with MIL-STD-882B.

In (8) Redesign/Control Actions, enter a brief description of the redesign/control/corrective action(s) necessary for the hazard condition being analyzed. Enter name(s) of related analysis/analyses and reference number(s).



Operating and Support Hazard Analysis (O&SHA).

The purpose of the O&SHA is to identify and analyze hazards associated with personnel and procedures during production, testing, installation, training, escape and operations.

The O&SHA is normally conducted on all identified hazards during tasks with man/machine interfaces. When the O&SHA indicates a potential problem, it should be made known to the responsible engineer in order to initiate a design review or a system safety working group action item. The O&SHA should be reviewed on a continuous basis to ensure that design modifications, procedures, testing, etc., do not create hazardous conditions.

The O&SHA helps ensure that corrective or preventive measures will be taken to minimize the possibility that any human error procedure will result in injury or system damage. The O&SHA provides inputs for recommendations of changes or improvements in design or procedures to improve efficiency and safety, development of warning and caution notes to be included in manuals and procedures, and the requirement for special training of personnel who operate and maintain the system.

A well-documented analysis shows compliance with the specified system safety and operational requirements.

TABLE B-5. OPERATING AND SUPPORT HAZARD ANALYSIS (O&SHA)

Instructions for Completing Form:

In Contract No. \_\_\_\_\_, enter the contract number for which O&SHA is being performed.

In Contractor \_\_\_\_\_, enter the name of the contractor responsible for the O&SHA.

In O&SHA No. \_\_\_\_\_, enter the O&SHA number which shall be coded and sequentially numbered by each contractor for each system. This coding sequence will be utilized for all related analyses.

In Revision No. \_\_\_\_\_, enter the revision number to indicate the latest status.

In Subsystem Function \_\_\_\_\_, enter the nomenclature and function of the subsystem as broken out from the system.

In System \_\_\_\_\_, enter the nomenclature of the applicable system.

In Facility \_\_\_\_\_, enter the description of the facility which includes the system.

In Drawing No. \_\_\_\_\_, enter the number of the drawing on which the function is indicated.

In Prepared by \_\_\_\_\_ Date \_\_\_\_\_, the preparer will sign and enter the date of review on each sheet of the analysis.

In Reviewed by \_\_\_\_\_ Date \_\_\_\_\_, the reviewer will sign and enter the date of review on each sheet of the analysis.

In Approved by \_\_\_\_\_ Date \_\_\_\_\_, the contractor's project manager will sign to approve and enter the date of approval on each sheet of the analysis.

In (1) Task or Operation, enter a brief description of the task or operation for which the hazard condition is being analyzed.

In (2) Potential Cause, enter the most likely primary and secondary causes of the hazard condition.

In (3) Effect(s) on Personnel System, enter a brief description of the hazard condition effect(s) related to personnel and/or system(s).

In (5) Hazard Category, enter the highest applicable hazard class in accordance with MIL-STD-882B.

In (6) Redesign/Control Actions, enter a brief description of the redesign/control/corrective action(s) necessary for the hazard condition being analyzed. Enter name(s) of related analysis/analyses and reference number(s).



## Fault Tree Analysis.

### Methodology.

Fault tree analysis is the functional development of a specified undesired event through logic statements of the causative conditions. The fault tree methodology involves the identification of a specific undesired event. A logic diagram, using established symbology for event and logic gate representation, is developed in which all events or system conditions which are considered necessary and sufficient to lead to the occurrence of the system event are identified and related logically to one another as they actually occur in the system. When this development is completed, the analyst is presented with a qualitative logic network in which all failure paths, both singular and multiple, and all combinations of events and conditions which could produce the undesired event are graphically represented.

The process can also be applied to a system phase as follows. The system operating modes are divided into phases. A phase is that increment of a system's life cycle which can be analyzed independently, yet recognizing that there can be commonality of analysis for any of the phases. A fault tree branch can be constructed separately for each phase. The fault tree development process for each phase should be logical and systematic.

Assuming the basic event relationships are well in hand, the development of the fault tree can proceed from the defined event by answering the following basic questions at each level:

- . Necessity
- . Sufficiency
- . Primary
- . Secondary
- . Command.

The two questions of "necessity" and "sufficiency" require an evaluation of fault event relationships to determine those system-unique events which are required to result in the end fault event. This logical process is followed whenever the coexistence of events through AND gates is required to result in the output event.

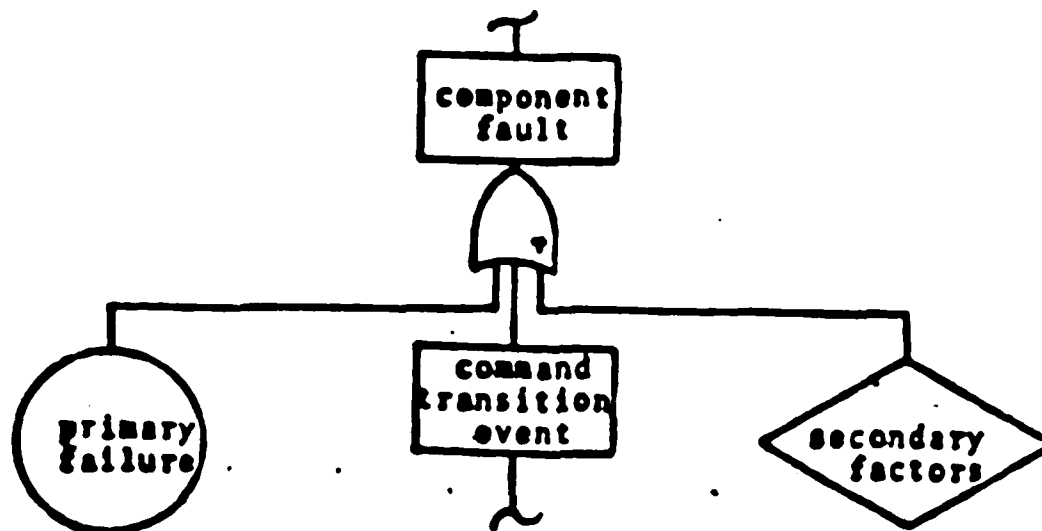
The three questions of "primary," "secondary," and "command" are guidelines for development at the ends of the branches. The analysis will normally be developed to the component level. At this detailed level of the fault tree, the following order of development should be followed:

1. Describe the component.
2. List all primary faults.
3. List all secondary factors for the equipment which are environment sensitive, i.e., those effects which can "cause" each primary fault mode.
4. Define the input or command event which basically is a normal sequence but occurs at the wrong time.




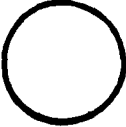
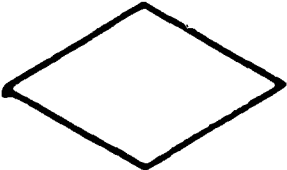





5. Repeat steps (2) and (3) for the event described by (4).
6. Continue this process to the appropriate level.

The resulting logic diagram to be constructed whenever a component fault has been identified is shown below. Each of the independent input events depicts a basic cause of the output event. It is the systematic utilization of the "command event" at this level of the analysis which allows the analyst to logically consider component interactions in the system.



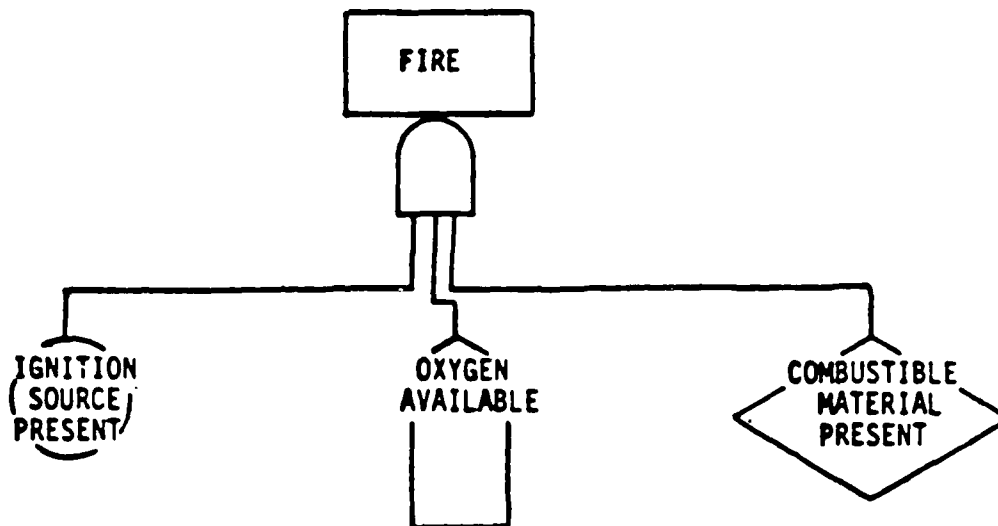
As the fault tree development progresses, it will be found that the above steps will occasionally be broken with the requirement that two events coexist before the development can continue. At this point, the questions of "necessity" and "sufficiency" must be satisfied.

TABLE B-6. FAULT TREE SYMBOLS

SYMBOL	DEFINITIONS
	An undesired or commanded event--will also describe the output of an "OR" or "AND" gate.
	A primary cause leading to an event, usually a malfunction of a component or specific circuit
	An event not developed because of insufficient information or consequence--sometimes called a secondary cause.
	The use of broken lines with the rectangle, circle, or diamond may be used to indicate a human interaction.
	An "OR" gate--this indicates that any of the events below the gate will lead to the event above gate.
	An "AND" gate--this indicates that all of the events below the gate must occur for the event above the gate to occur.
	A connecting symbol to another fault tree or fault tree section--number inside the triangle references another page in the fault tree.
	An event that can be expected to occur unless an abnormal event takes place.

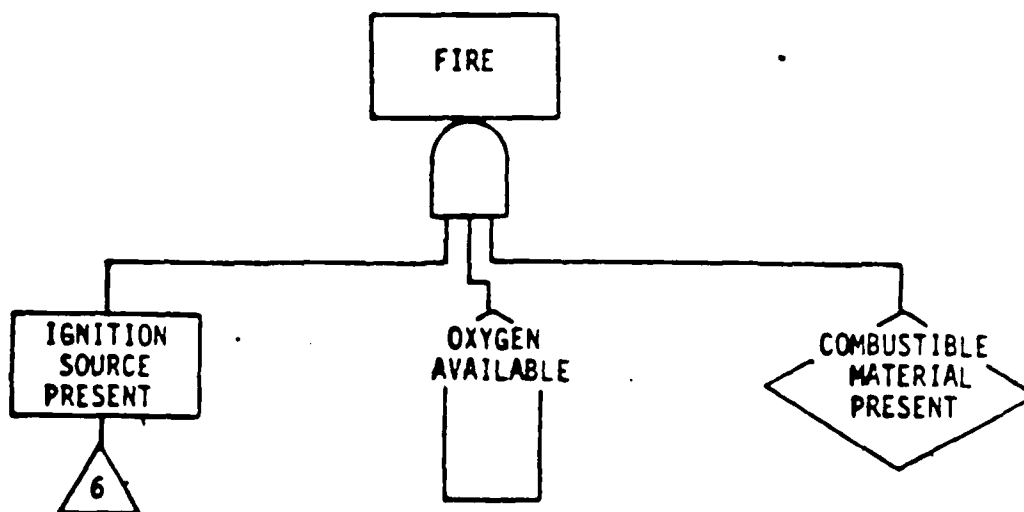
Constructing the Fault Tree.

As an example of the use of an AND gate, consider the undesired event, Fire. This event can occur if and only if the three events; ignition source present, oxygen available, and combustible material present coexist.



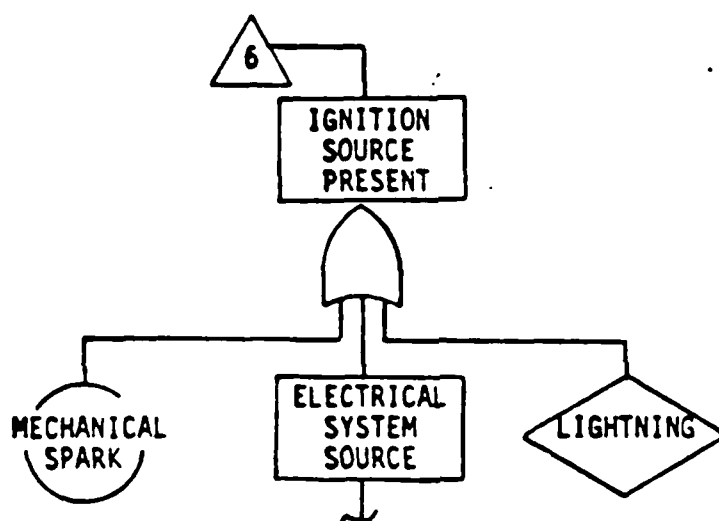
Thus "oxygen available" is represented as a house because by definition it is a condition normally expected to exist. "Combustible material present" for this example is not developed because of insufficient information.

This example can be carried a step further by considering "ignition source present" as an intermediate subsystem event rather than as a basic fault event. Replacing its circle by a rectangle gives the modified fault tree shown below.



The triangle labelled "6" below "ignition source present" is the transfer-in symbol. It is used when there is not more room on a given page to continue the analysis and, therefore, denotes that the continued analysis must be transferred in from another page.

Corresponding to the transfer-in symbol, there must always be a transfer-out symbol. The transfer-out symbol begins the continued analysis and is represented by a triangle with the line drawn out its side. It indicates that the continued analysis must be transferred out of that page and back into some previous page. The squiggled line beneath "electrical system failure" means that this event may be developed further but is not of particular interest for the development at hand. Notice also that in order to provide continuity the "ignition source present" rectangle is repeated below the transfer-out symbol.





## SUPPORT ACTIVITIES.

### General.

Throughout a system's life cycle there must be a continuing flow of information between disciplines. This is especially true for the safety and assurance disciplines. Next to design inadequacies and deficiencies, the principal causes of equipment and system failures and accidents are errors made during manufacturing and maintenance.

Much of the analytical work is complementary, and data developed for reliability purposes can be used in safety analyses. There is a continuous interplay that must be recognized during the analytical and investigatory processes. Some of these analyses are:

Failure modes and effects analysis (FMEA)

Failure modes, effects and criticality analysis (FMECA)

Logistics Supportability Analysis (LSA)

Predicted mean time to repair (PMTTR)

The FMECA and the PMTTR are discussed herein.

In addition, it is essential that the system safety engineer be able to track category I and II hazards and the verification of the eventual "fix," whether it be a design/hardware change, procedural change, or training requirement.

The critical items list (CIL) enables the engineer to do this.

### Critical Items List (CIL).

The purpose of the CIL is to compile all the identified safety-critical items to provide visibility for immediate corrective action to prevent personal injury or system damage when a category I or II hazard is identified. The CIL also provides a control technique for reliability when category I and II criticality items are identified. The CIL should be reviewed on a continuous basis until all items are resolved.

The CIL helps ensure that corrective action or preventive measures are taken to optimize system safety, reliability and maintainability by minimizing the magnitude and seriousness of those items which could result in personal injury, system damage and loss of operation, but which cannot be completely eliminated. The CIL provides inputs for recommending: changes or improvements in design; procedures to improve efficiency and safety; development of warning and caution notes to be included in manuals and procedures; requirements for special training; and management information for the operation and maintenance of the system. Those corrected CIL items should be incorporated into test programs to verify effectiveness of corrective measure(s).

Complete documentation shows compliance with the specified system safety and operational requirements.

## TABLE B-7. CRITICAL ITEMS LIST

Instructions for Completing Form:

In Contract No. \_\_\_\_\_, enter the contract number for which CIL is being performed.

In Contractor \_\_\_\_\_, enter the name of the contractor responsible for the CIL.

In CIL No. \_\_\_\_\_, enter the CIL number which shall be coded and sequentially numbered by each contractor. This coding sequence will be utilized for all related predictions and analyses.

In Revision No. \_\_\_\_\_, enter the revision number to indicate the latest status.

In Prepared by \_\_\_\_\_ Date \_\_\_\_\_, the preparer will sign and enter the date of issue or completion on each sheet.

- In Reviewed by \_\_\_\_\_ Date \_\_\_\_\_, the reviewer will sign and enter the date of review on each sheet.

In Approved by \_\_\_\_\_ Date \_\_\_\_\_, the contractor's project manager will sign to approve and enter the date of approval on each sheet.

In (1) LRU Description, enter nomenclature and brief functional description of the lowest replaceable unit.

In (2) Failure Reference Analysis, enter the applicable analysis name and number performed.

In (3) Failure Criteria Category, enter the highest applicable criticality category in accordance with the description in the glossary of terms.

In (4) Hazard Reference Analysis, enter the applicable hazard analysis name and number performed.

In (5) Hazard Category, enter the highest applicable hazard class in accordance with MIL-STD-882B and the description of the corrective action(s) or procedures which can be adopted to eliminate or minimize the effects or failure condition being analyzed.

In (6) Requirement, enter the specified safety and/or reliability guidelines.

In (7) Corrective Action, enter a brief description of the corrective actions necessary for the hazard condition analyzed.

In (8) Resolution, enter a brief description of final action taken to eliminate or control the hazard(s).

In (9) Retention Rationale, state the reasons for retaining the category I and II hazards as critical items 1 and 2.





## APPENDIX C

## INSPECTION/OBSERVATION CHECKLISTS

Planned Safety Inspection (PSI). All systems that are to be tested should be inspected prior to and following testing.

Safety Inspection Analysis (SIA). The SIA is a procedure for determining the safety requirements of a specific system or subsystem. It is a systematic assessment of a system to determine its inspection requirements. The SIA involves three basic steps:

Decide what items to inspect. Testers need to familiarize themselves with the systems they are to test. SARs and other documents should be used to develop a list of items to inspect as well as other analyses which may have been performed prior to the inspection. Such general categories as atmospheric conditions, structures, containers, electrical equipment, tools, hazardous material, pressurized equipment, power sources, structural openings, and safety devices are examples of items to be inspected.

Decide what item parts to inspect. Consideration should always be given to parts that are susceptible to damage, deterioration, stress, impact, vibration, etc.

Decide what conditions to look for. The inspectors must know what specific unsafe conditions to look for when they perform the inspections. There are dozens of one-word statements that tell the story (broken, loose, cracked, leaking, frayed, spalled, etc.). Sometimes it is necessary to describe a condition in a more precise detailed way (maximum pressure levels, minimum fluid levels, etc.).

A work sheet for developing an SIA is included in this Appendix (Fig. C-1). Assistance or consultation is available by contacting the safety office (system safety engineer).

TABLE C-1. SAMPLE WORK SHEET FOR SIA

SAFETY INSPECTION ANALYSIS		PROJECT: 1-VS-000-MBC-000 "Mobile Crane"	
		INSPECTOR: J. W. Doe	
INSPECTION ITEMS	PARTS TO INSPECT	CONDITIONS TO INSPECT FOR	FINDINGS
1. Crane structure	1a. Boom	Deformed, cracked, corroded members, loose bolts	
2. Hoist system	2a. Running ropes	Reduction in rope diameter, corrosion, number of broken wires, severe kinking, crushing	
	2b. Sheaves	Cracked, worn	
	2c. Hooks	Deformation, cracks, throat opening greater than 15°	

## CHECKLISTS

**MECHANICAL HAZARD CHECKLIST.** This checklist may be used as a guide for evaluating mechanical hazards when testing general equipment.

YES NO N/A

1. Is the equipment designed so that the center of gravity, configuration or location of legs and supports make the equipment unlikely to tip over from imbalance effects or strong wind?
2. Are expandable and collapsible structures such as shelters, jacks, supports, masts, tripods, etc., free from projections, sharp edges or design features which might be hazardous to personnel or associated equipment?
3. Are adequate lifting rings or slings provided for equipment which is normally moved or lifted by machine?
4. Are ladders, climbing rings, handholds, rails, walkways, etc., provided where needed?
5. Are steps and ladders and methods of supporting them safely made?
6. Are entrances to equipment shelters free of hazardous obstructions?
7. Do floor surfaces have adequate nonslip characteristics?
8. Are fasteners and methods of securing equipment to walls and racks sufficiently strong to prevent breakaway and falling?
9. Can equipment shelters mounted on vehicles be entered without encountering a hazard?
10. Does the installation of equipment on vehicles provide sufficient mechanical strength to minimize potential safety hazards?
11. Are provisions made in vehicular and shelter installations for securing equipment, tools and accessories during movement?
12. Are safety measures provided in the event the trailer becomes detached from the towing vehicle?
13. When semitrailers are detached from towing vehicles do dolly wheels or landing gear provide adequate support?
14. If a standard military vehicle has been modified to accommodate the equipment, is the vehicle still capable of satisfactory and safe operation?

YES NO N/A

15. Do doors and hinged covers have positive-action hold-open devices?
16. Are locking mechanisms for doors and drawers designed to prevent injury to the operator when the lock is released?
17. Are limit stops provided on roll-out racks and drawers?
18. Are there provisions for easily overriding limit stops on roll-out racks and drawers?
19. Is the method of opening a cover evident from the construction of the cover? If not, is an instruction plate permanently attached to the outside of the cover?
20. Is it evident when a cover is in place but not secured?
21. Is the equipment provided with suitable carrying handles?
22. Are handles recessed rather than extended where they might be hazardous?
23. Are handles positioned so they cannot catch on other units, wiring, or protrusions?
24. Are handles located over center of gravity whenever possible?
25. Are doors and other openings free of hazards from improperly designed catches, hinges, supports, fasteners and stops?
26. Are components placed to allow sufficient space for use of test equipment and tools?
27. Are heavy parts located as close as possible to load-bearing structures and as low as possible?
28. Is the weight distribution such that the equipment is easy to handle, move or position?
29. Are tasks of operation and maintenance such that they do not require excessive physical strength?
30. When the equipment is to be manpacked are the weight and configuration such that the combat effectiveness of the test soldier is not jeopardized?
31. Is the equipment free of sharp or overhanging edges and corners that might cause injury to personnel?
32. When glass is used is it glareproof and shatterproof?

YES NO N/A

33. Do exposed gears, cams, levers, fans, belts or other reciprocating, rotating or moving parts have adequate safety covers?
34. Is the equipment provided with sufficient caution plates to warn maintenance personnel of potential safety hazards?
35. Are warning signs coded and colored in accordance with Army regulations?
36. When required are provisions made for protection against eye hazards from flying particles?
37. Are safety valves, relief valves or other safety devices adjusted to their proper settings?
38. Are potential mechanical hazards adequately treated in the instructional manual?

ELECTRICAL HAZARD CHECKLIST. This checklist may be used as a guide for evaluating electrical or electronic hazards when testing general equipment.

YES NO N/A

1. Is the path to ground from the equipment continuous and permanent?
2. Does the grounding system have sufficient mechanical strength to minimize the possibility of accidental ground disconnection?
3. Is the ground connection to the chassis or frame mechanically secured by one of the following methods?
  - a. Secured to a spot-welded terminal lug.
  - b. Secured to a portion of the chassis or frame that has been formed into a soldering lug.
  - c. Secured by a screw or nut and a lockwasher to a terminal on the ground wire.
4. Is the grounding system of sufficient gauge size to conduct safely any currents that may be imposed upon it?
5. Is the impedance of the ground system sufficiently low to limit the potential above ground and to facilitate the operation of the overcurrent devices in the circuits?
6. Are ground connections to shields and other mechanical parts, except the chassis and frame, made independently of the electrical circuits?

YES NO N/A

7. Do plugs and convenience outlets for use with portable tools and equipment have provisions for automatic grounding?
8. Are all external metal parts, control shafts, bushings and shields at ground potential at all times?
9. Are voltages properly marked?
10. Are guards, safety covers and warning plates provided for items handling 70 to 500 volts rms or DC?
11. Are built-in test points provided where measurements of potentials are greater than or equal to 300 volts peak?
12. Can high-voltage circuits and capacitors be discharged to 30 volts within 2 seconds or less by automatic protective devices?
13. When equipment is designed to operate on more than one type input power, are adequate precautions taken to prevent connection of improper power?
14. Are DC power connections clearly marked for polarity?
15. Are adjustment screws or other commonly worked-on parts located away from unprotected high voltages?
16. Are tools to be used near high voltages adequately insulated?
17. Do meters have protection against high voltage or current at the terminals?
18. Are compartments operating at potentials in excess of 500 volts rms or DC where access is required for adjustment purposes equipped with interlocks with by-pass devices which remove all potentials in excess of 30 volts rms or DC?
19. In compartments where access into the interior is required for adjustment purposes and no interlocks are used, are voltages in excess of 70 volts rms or DC isolated with barriers or guards?
20. Is the grounding conductor of the equipment electrically insulated from the AC power return (neutral) within the system and/or equipment?
21. Are mechanical and electrical interlocks designed to prevent energizing by movement when men are in positions where it could be dangerous?

YES NO N/A

22. Are internal controls located at safe distances from dangerous voltages?
23. Are physically similar but electrically noninterchangeable components keyed so that it is impossible to insert a wrong unit?
24. Where design considerations require plugs and receptacles of similar configuration, are mating plugs and receptacles suitably coded and marked?
25. Is shielding sufficiently separated from exposed conductors to prevent shorting or arcing?
26. Are wires and cables adequately supported and terminated to prevent shock and fire hazard?
27. Are wires and cables properly protected at points where they pass through metal partitions?
28. Can maintenance be accomplished with shielding in place?
29. Do floor surfaces have adequate insulating characteristics?
30. Are emergency controls placed in readily accessible positions?
31. Is the main power breaker in an easily accessible location?
32. Does the main power breaker cut off all power to the complete equipment or system?
33. Can the power be cut off while installing, replacing or interchanging complete equipment, an assembly or part thereof?
34. Are safety switches provided which will deactivate associated mechanical drive units without disconnecting other parts of the equipment?
35. Are remotely located assemblies provided with safety switches to allow independent disconnection of the equipment?
36. Are potential electrical hazards adequately treated in the instruction manual?
37. Are disconnect devices (circuit breakers) properly labeled?

**CHEMICAL HAZARD CHECKLIST.** This checklist may be used as a guide when testing general equipment which uses chemicals.

YES NO N/A

1. Has each chemical used in or with the system been identified in the safety assessment report?

YES NO N/A

2. Have approved time-concentration exposure limits been established for each chemical used? If not, are toxicity tests being performed and interim safety precautions provided by the Surgeon General?
3. Has each condition necessary for personnel exposure or release to atmosphere or water been evaluated?
4. Are the time-concentration exposure limits to personnel exceeded during operation of the item?
5. Are precautions made to prevent exposure to respiratory hazards adequate? Skin absorption? Ingestion?
6. Have all possible chemical reactions between the materials involved been analyzed including those with materials used in conjunction with the item being tested.
7. Are operator means of detecting a hazardous condition adequate?
8. Are all harmful chemicals properly identified with appropriate caution notices?
9. Are adequate safety devices and safety instructions provided for handling and use of gases stored under high pressure and/or extremely low temperature?
10. Has the effect of decontamination procedures on the equipment surface been studied? Is chemical or biological material retained in the paint or material? What is the desorption rate?
11. Did any personnel suffer irritation dermatitis as a result of contact with the chemical materials?
12. Are air intakes isolated from the exhaust?
13. Are adequate oxygen levels maintained inside shelters, etc.?
14. Is the collective efficiency of material collection equipment (scrubbers, filters, incinerators) adequate to prevent hazardous conditions?
15. Are the safeguards in event of power outage adequate?
16. Are adequate disposal procedures provided for all chemicals used as part of or with the item?



## PHYSIOLOGICAL HAZARDS CHECKLIST.

YES NO N/A

1. Is the ambient noise level acceptable for personnel safety and efficiency?
2. Have all physical operator stresses such as repetitive motions, awkward working conditions, and vibration been evaluated?
3. Have all mental demands on operators been evaluated?
4. Have all lifting and carrying requirements been evaluated?
5. When necessary, have all ear- and eye-protection devices been provided?
6. Are adequate controls and warning signs included to prevent exposure to ionizing radiation in excess of standards?
7. Are adequate controls and warning signs included to prevent exposure to nonionizing radiation, including UV, IR, laser, and microwave in excess of standards?
8. Are adequate illumination levels available for the tasks required?
9. Has heat stress to personnel as the result of exposure to high temperature or wearing protective equipment been evaluated?
10. Does the ventilating system provide for operator safety by ducting excess heat liberated by equipment to the outside of the shelter?
11. Is equipment-cooling air for shelter-mounted equipment completely separated from the personnel space to prevent contamination of the surrounding air?
12. Are adequate precautions made to prevent exposure of personnel to respiratory hazards from toxic gases, ducts, fumes and mists?
13. Is the air intake isolated from the exhaust?
14. Is the shelter heating and ventilating system designed to safeguard against depletion of oxygen in the personnel area?
15. Are all air-flow paths free of obstructions?

YES NO N/A

16. Is shelter-mounted equipment furnished with test kits for checking air contamination and oxygen depletion?
17. Are acids or other harmful liquids properly identified with appropriate caution notices?
18. Do instructions specify type of cleaning fluid and precautions to be taken when cleaning equipment?
19. Are adequate safety devices and safety instructions provided for handling and use of gases stored under high pressure and/or extreme temperatures, e.g., hydrogen, helium, oxygen, nitrogen?
20. Is protection provided against hot surfaces which might be dangerous to personnel?

## FIRE AND EXPLOSION HAZARD CHECKLIST.

YES NO N/A

1. Have all possible ignition sources been evaluated to determine potential hazard?
2. Has the flammability of the materials been taken into account in planning for use of the item?
3. Are fire extinguishers of the proper type for the equipment provided and mounted in easily accessible locations?
4. Are properly marked fire exits provided in shelters when required?
5. Have precautions been taken to ensure that the storage and distribution of flammable material are done safely?
6. Is a self-closing metal can provided for oily rags and waste where required?
7. Have fire-extinguishing methods been included in technical publications?

APPENDIX D  
HAZARD SEVERITY AND CLASSIFICATION (from MIL-STD-882B)

**Hazard Severity.** Hazard severity categories are defined to provide a qualitative measure of the worst credible mishap resulting from personnel error; environmental conditions; design inadequacies; procedural deficiencies; or system, subsystem or component failure or malfunction as follows:

Description	Category	Mishap Definition
CATASTROPHIC	I	Death or system loss
CRITICAL	II	Severe injury, severe occupational illness, or major system damage
MARGINAL	III	Minor injury, minor occupational illness, or minor system damage
NEGLECTIBLE	IV	Less than minor injury, occupational illness, or system damage

These hazard severity categories provide guidance to a wide variety of programs. Adaptation to a particular program, however, is generally required to provide a mutual understanding between the MA and the contractors as to the meaning of the terms used in the category definitions. The adaptation must define what constitutes system loss, major or minor system damage, and severe and minor injury and occupational illness.

**Hazard Probability.** The probability that a hazard will be created during the planned life expectancy of the system can be described in potential occurrences per unit of time, events, population, items, or activity. Assigning a quantitative hazard probability to a potential design or procedural hazard is generally not possible early in the design process. A qualitative hazard probability may be derived from research, analysis, and evaluation of historical safety data from similar systems. Supporting rationale for assigning a hazard probability shall be documented in hazard analysis reports. An example of a qualitative hazard probability ranking is:

Description*	Level	Specific Individual Item	Fleet or Inventory**
FREQUENT	A	Likely to occur frequently	Continuously experienced
PROBABLE	B	Will occur several times in life of an item	Will occur frequently
OCCASIONAL	C	Likely to occur sometime in life of an item	Will occur several times
REMOTE	D	Unlikely but possible to occur in life of an item	Unlikely but can reasonably be expected to occur
IMPROBABLE	E	So unlikely, it can be assumed occurrence may not be experienced	Unlikely to occur, but possible

\*Definitions of descriptive words may have to be modified based on quantity involved.

\*\*The size of the fleet or inventory should be defined.

7 April 1986

TOP 1-1-060

TABLE D-1. HAZARD CLASSIFICATION GUIDELINES (from TOP 1-1-012)

HAZARD PROBABILITY				
	FREQUENT	PROBABLE	OCCASIONAL	REMOTE
SPECIFIC INDIVIDUAL ITEM	Likely to occur frequently	Will occur several times in life of item	Likely to occur sometime in the life of item	Unlikely but possible to occur in the life of item
	Continuously experienced	Will occur frequently	Will occur several times	Unlikely but can reasonably be expected to occur
FLEET OR INVENTORY				
HAZARD SEVERITY				
	A	B	C	D
CATASTROPHIC - May cause death or system loss	I DEFICIENCY	DEFICIENCY	DEFICIENCY	DEFICIENCY
				SHORTCOMING
CRITICAL - May cause severe injury, severe occupational illness, or major system damage	II DEFICIENCY	DEFICIENCY	DEFICIENCY	SHORTCOMING
				SUGGESTED IMPROVEMENT
MARGINAL - May cause minor injury, minor occupational illness, or minor system damage	III DEFICIENCY	SHORTCOMING	SHORTCOMING	SUGGESTED IMPROVEMENT
				OR ACCEPTABLE
NEGLECTIBLE - May cause less than minor injury, occupational illness, or system damage	IV SHORTCOMING	SUGGESTED IMPROVEMENT	ACCEPTABLE	ACCEPTABLE

APPENDIX E  
SAFETY-RELATED TOPS

NUMBER	TITLE
1-1-012	Classification of Deficiencies and Shortcomings and Changes 1, 2, 3
1-1-019	Testing Armament and Individual Weapons and Change 1
1-1-051	Ammunition and Explosives
1-1-056	Software Testing
1-2-500	Transportability and Changes 1, 2, 3
1-2-502	Durability
1-2-504	Physical Characteristics
1-2-511	Electromagnetic Compatibility Requirements, Systems Testing
1-2-608	Sound Level Measurements
1-2-610	Human Factors Engineering (Part I, Part II)
1-2-612	Nuclear Radiation Effects
1-2-613	Nuclear Effects Tests of Army Materiel (Blast)
2-2-508	Automotive Safety and Health Hazard Evaluation
2-2-601	Electrical Systems (Vehicle and Weapon Subsystems)
2-2-608	Braking, Wheeled Vehicles and Changes 1, 2
2-2-609	Steering
2-2-610	Gradeability and Slide Slope Performance
2-2-614	Toxic Hazards Tests for Vehicles and Other Equipment
2-2-627	Braking - Tracked Vehicles
2-2-704	Tires
2-2-800	Center of Gravity
2-4-003	Wheeled, Tracked and General Purpose Vehicles
3-1-002	Confidence Intervals and Sample Size
3-1-005	Field Artillery Statistics
3-2-500	Weapon Characteristics

3-2-503	Safety Evaluation of Fire Control Systems - Electrical and Electronic Equipment and Change 1
3-2-504	Safety Evaluation of Hand and Shoulder Weapons
3-2-616	Radio Frequency Radiation Hazards to Personnel
3-2-711	Safety Evaluation - Radioactive Components of Materiel
3-2-805	Safety Evaluation of Cannon and Recoilless Weapons
4-2-502	Safety Evaluation of Mines and Demolitions
4-2-504	Safety Testing of Artillery, Mortar, and Recoilless Rifle Ammunition and Change 1
4-2-504(2)*	Safety Evaluation of Tank Ammunition
4-2-705	Cartridge Cases
5-2-619	Safety Testing of Missile, Rocket, and Guided Projectile Employing Manned Launch Stations
6-2-507	Safety and Health Evaluation - Communication/Electronic Equipment
7-2-506	Airdrop Systems Safety
7-3-506(P)	Safety (Aviation Materiel)
8-2-113	Breathing Apparatuses, Self-Contained Air/Oxygen Supply
10-2-051	Fire Extinguishers
10-2-508	Safety and Health Hazard Evaluation - General Equipment

\*International Test Operations Procedure (ITOP)

## APPENDIX F

## REFERENCES

Required References

1. AR 70-10. Test and Evaluation During Development and Acquisition of Materiel, 29 August 1975.
2. TECOM Pamphlet 310-4, Military Publications - Index of Test Operations Procedures, 31 January 1984.
3. TECOM Regulation 70-24, Research, Development, and Acquisition-- Documenting TECOM Testing, 22 June 1981.
4. AR 385-16, System Safety Engineering and Management, 3 September 1985; DARCOM Supplement 1, 22 January 1982; TECOM Supplement 1, 11 June 1982; APG Supplement 1, 5 January 1983.
5. AR 40-10 Health Hazard Assessment Program in Support of the Army Materiel Acquisition Decision Process, 15 September 1983.
6. MIL-STD-882B, System Safety Program Requirements, 30 March 1984.
7. MIL-STD-454J, Standard General Requirements for Electronic Equipment, 30 April 1984; Notice 1, 30 August 1984; Notice 2, 1 March 1985.
8. TECOM Regulation 385-7, Potential Health Hazards to Humans Participating in Testing, 15 November 1978.
9. TOP 2-2-614, Toxic Hazards Tests for Vehicles and Other Equipment, 14 December 1984.
10. AMC Regulation 385-100, Safety Manual, 17 August 1981.
11. AR 70-1 Army Research, Development, and Acquisition - System Acquisition Policy and Procedures, 1 February 1984; Change 1, 15 July 1984.
12. TOP 1-1-056, Software Testing, 15 November 1977.
13. AMC Pamphlet 706-110 through -114, Engineering Design Handbook - Experimental Statistics, 16, 12, 12, 16, and 17 December 1969, respectively.
14. MTP 3-1-002, Confidence Intervals and Sample Size, 25 January 1967.

References for Information Only

NONE